

“Express Mail” Mailing Label No. **EL436467793US**

**PATENT APPLICATION
ATTORNEY DOCKET NO. NA00-13501**

5

10

**METHOD AND APPARATUS FOR
FACILITATING SECURE ANONYMOUS
EMAIL RECIPIENTS**

15

Inventor: William F. Price III

20

BACKGROUND

25

Field of the Invention

The present invention relates to computer security and electronic mail. More specifically, the present invention relates to a method and an apparatus for facilitating transmission of an encrypted electronic mail message to anonymous recipients without divulging the identities of the anonymous recipients.

Related Art

The advent of computer networks has led to an explosion in the development of applications that facilitate rapid dissemination of information. In particular, electronic mail (email) is becoming the predominant method for

00000000000000000000000000000000

communicating textual and other non-voice information. Using email, it is just as easy to send a message to a recipient on another continent as it is to send a message to a recipient within the same building. Furthermore, an email message typically takes only minutes to arrive, instead of the days it takes for conventional
5 mail to snake its way along roads and through airports.

One problem with email is that it is hard to ensure that sensitive information sent through email is kept confidential. This is because an email message can potentially traverse many different computer networks and many different computer systems before it arrives at its ultimate destination. An
10 adversary can potentially intercept an email message at any of these intermediate points along the way.

One way to remedy this problem is to "encrypt" sensitive data using an encryption key so that only someone who possesses a corresponding decryption key can decrypt the message. (Note that for commonly used symmetric
15 encryption mechanisms the encryption key and the decryption key are the same key.) A person sending sensitive data through email can encrypt the sensitive data using the encryption key before it is sent through email. At the other end, the recipient of the email can use the corresponding decryption key to decrypt the sensitive information.

20 Encryption works well for a message sent to a single recipient. However, encryption becomes more complicated for a message sent to multiple recipients. This is because encryption keys must be managed between the sender and the multiple recipients.

Conventional mail protocols, such as the Pretty Good Privacy (PGP)
25 protocol, send mail to multiple recipients by encrypting a message with a session key (that is randomly selected for the message) to form an encrypted message. The session key is then encrypted with the public key of each of the recipients to

form a set of encrypted keys. This set of encrypted keys is sent with the encrypted message to all of the recipients. Each recipient uses one of its private keys to decrypt an encrypted session key and then uses the session key to decrypt the encrypted message.

5 Note that key identifiers for the public keys that were used to encrypt the encrypted session keys are sent along with the encrypted session keys, so that each recipient can determine whether or not the recipient possesses a corresponding private key that can decrypt the encrypted session key. These identifiers are typically generated by computing as a hash of the public key.

10 Unfortunately, the key identifiers can also identify a recipient of an email message to other recipients of the email message. This complicates the process of sending an encrypted email message to anonymous recipients, because the recipients of the email message can determine the identities of the anonymous recipients by examining the key identifiers for the anonymous recipients.

15 What is needed is a method and an apparatus for facilitating transmission of encrypted email to anonymous recipients without divulging the identities of the anonymous recipients.

SUMMARY

20 One embodiment of the present invention provides a system that facilitates secure transmission of an email message to anonymous recipients without divulging the identities of the anonymous recipients. This system constructs an email message by identifying recipients of the email message. These recipients can include known recipients, who can be identified by examining the email message, and anonymous recipients, who cannot be identified by examining the email message. The system also generates a session key for the email message, and encrypts a body of the email message with the session key. The system also

creates a recipient block for the email message that contains an entry for each recipient of the email message. Each entry in this recipient block contains the session key encrypted with a public key associated with the recipient to form an encrypted session key, so that only a corresponding private key held by the
5 recipient can be used to decrypt the encrypted session key. Each entry additionally contains an identifier for the associated public key, so that each recipient can determine whether the recipient possesses a corresponding private key that can decrypt the encrypted session key. These identifiers are constructed so that identifiers for public keys belonging to known recipients are statistically
10 unique, and identifiers for public keys belonging to anonymous recipients are not statistically unique. Finally, the system sends the email message to the recipients.

In one embodiment of the present invention, identifiers for public keys belonging to anonymous recipients provide only enough information to exclude a large percentage of all possible corresponding private keys from being able to
15 decrypt the body of the email message.

In one embodiment of the present invention, an identifier for a public key is formed by creating a hash of the public key.

In one embodiment of the present invention, an identifier for a public key belonging to an anonymous recipient is additionally modified so the identifier is
20 not statistically unique. In this way, the identifier cannot be used to uniquely identify the anonymous recipient. However, a recipient can use the identifier to exclude a large percentage of all possible corresponding public keys held by the recipient from matching the identifier.

In one embodiment of the present invention, prior to encrypting the body
25 of the email message, the system includes a checksum into the body of the email message, so that a recipient can examine the checksum to verify that the correct private key was used in decrypting the email message.

One embodiment of the present invention provides a system that facilitates secure transmission of an email message to anonymous recipients without divulging the identities of the anonymous recipients. This system operates by receiving the email message at a recipient. This email message includes a message body that has been encrypted with a session key. It also includes a recipient block that contains an entry for each recipient of the email message. Each of these entries contains the session key encrypted with a public key associated with the recipient to form an encrypted session key. Each entry additionally contains an identifier for the associated public key, wherein identifiers for public keys belonging to known recipients are statistically unique, and identifiers for public keys belonging to anonymous recipients are not statistically unique. Next, the system attempts to match a candidate public key held by the recipient with key identifier in the recipient block. If the candidate public key matches a key identifier, the system decrypts the associated encrypted session key using an associated private key to restore the session key, and then decrypts the message body using the session key. The system then examines a checksum in the message body to verify that message body was correctly decrypted.

20

BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 illustrates the transmission of an email message from a sender to recipients across a network in accordance with an embodiment of the present invention.

25

FIG. 2 illustrates the structure of an encrypted email message in accordance with an embodiment of the present invention.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
279
280
281
282
283
284
285
286
287
288
289
289
290
291
292
293
294
295
296
297
298
299
299
300
301
302
303
304
305
306
307
308
309
309
310
311
312
313
314
315
316
317
318
319
319
320
321
322
323
324
325
326
327
328
329
329
330
331
332
333
334
335
336
337
338
339
339
340
341
342
343
344
345
346
347
348
349
349
350
351
352
353
354
355
356
357
358
359
359
360
361
362
363
364
365
366
367
368
369
369
370
371
372
373
374
375
376
377
378
379
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
10010
10011
10012
10013
10014
10015
10016
10017
10018
10019
10020
10021
10022
10023
10024
10025
10026
10027
10028
10029
10030
10031
10032
10033
10034
10035
10036
10037
10038
10039
10040
10041
10042
10043
10044
10045
10046
10047
10048
10049
10050
10051
10052
10053
10054
10055
10056
10057
10058
10059
10059
10060
10061
10062
10063
10064
10065
10066
10067
10068
10069
10069
10070
10071
10072
10073
10074
10075
10076
10077
10078
10079
10079
10080
10081
10082
10083
10084
10085
10086
10087
10088
10089
10089
10090
10091
10092
10093
10094
10095
10096
10097
10098
10099
10099
100100
100101
100102
100103
100104
100105
100106
100107
100108
100109
100110
100111
100112
100113
100114
100115
100116
100117
100118
100119
100119
100120
100121
100122
100123
100124
100125
100126
100127
100128
100129
100129
100130
100131
100132
100133
100134
100135
100136
100137
100138
100139
100139
100140
100141
100142
100143
100144
100145
100146
100147
100148
100149
100149
100150
100151
100152
100153
100154
100155
100156
100157
100158
100159
100159
100160
100161
100162
100163
100164
100165
100166
100167
100168
100169
100169
100170
100171
100172
100173
100174
100175
100176
100177
100178
100179
100179
100180
100181
100182
100183
100184
100185
100186
100187
100188
100189
100189
100190
100191
100192
100193
100194
100195
100196
100197
100198
100199
100199
100200
100201
100202
100203
100204
100205
100206
100207
100208
100209
100209
100210
100211
100212
100213
100214
100215
100216
100217
100218
100219
100219
100220
100221
100222
100223
100224
100225
100226
100227
100228
100229
100229
100230
100231
100232
100233
100234
100235
100236
100237
100238
100239
100239
100240
100241
100242
100243
100244
100245
100246
100247
100248
100249
100249
100250
100251
100252
100253
100254
100255
100256
100257
100258
100259
100259
100260
100261
100262
100263
100264
100265
100266
100267
100268
100269
100269
100270
100271
100272
100273
100274
100275
100276
100277
100278
100279
100279
100280
100281
100282
100283
100284
100285
100286
100287
100288
100289
100289
100290
100291
100292
100293
100294
100295
100296
100297
100298
100299
100299
100300
100301
100302
100303
100304
100305
100306
100307
100308
100309
100309
100310
100311
100312
100313
100314
100315
100316
100317
100318
100319
100319
100320
100321
100322
100323
100324
100325
100326
100327
100328
100329
100329
100330
100331
100332
100333
100334
100335
100336
100337
100338
100339
100339
100340
100341
100342
100343
100344
100345
100346
100347
100348
100349
100349
100350
100351
100352
100353
100354
100355
100356
100357
100358
100359
100359
100360
100361
100362
100363
100364
100365
100366
100367
100368
100369
100369
100370
100371
100372
100373
100374
100375
100376
100377
100378
100379
100379
100380
100381
100382
100383
100384
100385
100386
100387
100388
100389
100389
100390
100391
100392
100393
100394
100395
100396
100397
100398
100399
100399
100400
100401
100402
100403
100404
100405
100406
100407
100408
100409
100409
100410
100411
100412
100413
100414
100415
100416
100417
100418
100419
100419
100420
100421
100422
100423
100424
100425
100426
100427
100428
100429
100429
100430
100431
100432
100433
100434
100435
100436
100437
100438
100439
100439
100440
100441
100442
100443
100444
100445
100446
100447
100448
100449
100449
100450
100451
100452
100453
100454
100455
100456
100457
100458
100459
100459
100460
100461
100462
100463
100464
100465
100466
100467
100468
100469
100469
100470
100471
100472
100473
100474
100475
100476
100477
100478
100479
100479
100480
100481
100482
100483
100484
100485
100486
100487
100488
100489
100489
100490
100491
100492
100493
100494
100495
100496
100497
100498
100499
100499
100500
100501
100502
100503
100504
100505
100506
100507
100508
100509
100509
100510
100511
100512
100513
100514
100515
100516
100517
100518
100519
100519
100520
100521
100522
100523
100524
100525
100526
100527
100528
100529
100529
100530
100531
100532
100533
100534
100535
100536
100537
100538
100539
100539
100540
100541
100542
100543
100544
100545
100546
100547
100548
100549
100549
100550
100551
100552
100553
100554
100555
100556
100557
100558
100559
100559
100560
100561
100562
100563
100564
100565
100566
100567
100568
100569
100569
100570
100571
100572
100573
100574
100575
100576
100577
100578
100579
100579
100580
100581
100582
100583
100584
100585
100586
100587
100588
100589
100589
100590
100591
100592
100593
100594
100595
100596
100597
100598
100599
100599
100600
100601
100602
100603
100604
100605
100606
100607
100608
100609
100609
100610
100611
100612
100613
100614
100615
100616
100617
100618
100619
100619
100620
100621
100622
100623
100624
100625
100626
100627
100628
100629
100629
100630
100631
100632
100633
100634
100635
100636
100637
100638
100639
100639
100640
100641
100642
100643
100644
100645
100646
100647
100648
100649
100649
100650
100651
100652
100653
100654
100655
100656
100657
100658
100659
100659
100660
100661
100662
100663
100664
100665
100666
100667
100668
100669
100669
100670
100671
100672
100673
100674
100675
100676
100677
100678
100679
100679
100680
100681
100682
100683
100684
100685
100686
100687
100688
100689
100689
100690
100691
100692
100693
100694
100695
100696
100697
100698
100699
100699
100700
100701
100702
100703
100704
100705
100706
100707
100708
100709
100709
100710
100711
100712
100713

002001-26242960

Transmission of Email Message

FIG. 1 illustrates the transmission of an email message 104 from a sender 102 to recipients 108-110 across a network 106 in accordance with an embodiment of the present invention. Network 106 can include any type of wire or wireless communication channel capable of coupling together computing nodes. This includes, but is not limited to, a local area network, a wide area network, or a combination of networks. In one embodiment of the present invention, network 106 includes the Internet.

10 Sender 102 can include any type of computing system that can send an email message, while recipients 108-110 can include any type of computing systems that can receive an email message.

Recipients 108-110 hold private keys 112-114, respectively. These private keys 112-114 enable recipients 108-110 to decrypt email messages that have been encrypted with corresponding public keys.

15 Note that knowledge of a public key cannot be used to decrypt a message encrypted with the public key. The corresponding private key must be used, and this private key is typically kept in secrecy by recipients 108-110.

The system illustrated in FIG. 1 operates generally as follows. Sender 102 produces an email message, the body of which is encrypted with a session key. 20 This session key is encrypted with the public key of each of the recipients. Next, the encrypted message and the encrypted session key are sent to recipients 108-110 across network 106. Recipients 108-110 use their private keys 112-114 to decrypt the encrypted session key, and then use the session key to decrypt the body of the email message.

25

Structure of Email Message

FIG. 2 illustrates the structure of an encrypted email message 104 in accordance with an embodiment of the present invention. Email message 104 includes an encrypted message body 206 containing information to be communicated to from sender 102 to recipients 108-110. Encrypted message body 206 is created by first producing a checksum (otherwise known as a hash or a message digest) of the message body and then encrypting the message body with a session key. This session key can be randomly generated by the sender for the message.

Email message 104 also includes a recipient block 204 containing an entry for each recipient of email message 104. In FIG. 2, recipient block 204 contains three entries 220-222 for each of three recipients 108-110 of email message 104.

Each entry contains an encrypted session key and a key ID. More specifically: entry 220 contains encrypted session key 214 and key ID 210; entry 221 contains encrypted session key 216 and key ID 211; and entry 222 contains encrypted session key 218 and key ID 212.

Each encrypted session key is formed by encrypting the session key for the message with a public key belonging to a recipient so that the encrypted session key can be decrypted with a corresponding private key of the recipient. For example, if entry 220 is for recipient 108, encrypted session key 214 is formed by encrypting the session key with a public key belonging to recipient 108. This enables recipient 108 to decrypt the encrypted session key with a corresponding private key held by recipient 108.

Each key ID is formed by taking a hash of the public key that was used to encrypt the associated encrypted session key. For example, if entry 220 corresponds to recipient 108, key ID 210 is formed by taking a hash of the public key for recipient 108. Key ID 210 can then be used by recipient 108 to determine

00000000-0000-0000-0000-000000000000

whether recipient 108 possesses the corresponding private key within private keys 112 to decrypt encrypted session key 214.

Note that key ID 210 is typically long, for example 64 bits. This ensures that key ID 210 is statistically unique – although uniqueness cannot be guaranteed 5 because there exists an almost non-existent probability that two different public keys will result in the same 64-bit hash.

Entry 222 corresponds to an anonymous recipient 110, who cannot be identified by examining the email message. In order to protect the identity of anonymous recipient 110, key ID 212 is truncated to a small number of bits; for 10 example, three to six bits. In this way, key ID 212 cannot be used to uniquely identify anonymous recipient 110. However, anonymous recipient 110 can use the key identifier 212 to exclude a large percentage of all possible corresponding private keys 114 held by recipient 110 from matching the identifier. Hence, if anonymous recipient 110 possesses a private key to decrypt encrypted session key 15 218, anonymous recipient 110 must try at most a small number of its private keys to determine if it possesses the proper private key. Without truncated key ID 212, anonymous recipient 110 may potentially have to try all of its private keys 114.

Process of Generating an Encrypted Email Message

20 FIG. 3 is a flow chart illustrating the process of generating an encrypted email message 104 at sender 102 in accordance with an embodiment of the present invention. The system starts by identifying recipients of email message 104 (step 302). These recipients can include known recipients, who can be identified by examining the email message, and anonymous recipients, who 25 cannot be identified by examining the email message. The system also generates a session key for the email message (step 304). This session key can be generated randomly by sender 102.

The system additionally generates checksum 208 for the email message body using some type of hashing mechanism (step 306). The system then encrypts the message body and the checksum to form encrypted message body 206 (step 308).

5 The system also creates recipient block 204 for email message 104 (step 310). Each of the entries 220-222 in recipient block 204 contain the session key encrypted with a public key associated with the corresponding recipient to form an encrypted session key. This ensures that only a corresponding private key held by the recipient can be used to decrypt the encrypted session key.

10 Each entry additionally contains an identifier for the associated public key, so that each recipient can determine whether the recipient possesses a corresponding private key that can decrypt the encrypted session key. These identifiers are constructed so that identifiers for public keys belonging to known recipients are statistically unique, for example by using a hashing mechanism.

15 Identifiers for public keys belonging to anonymous recipients are modified so that they are not statistically unique; for example by truncating the hash to a small number of bits. Finally, the system sends the email message to the recipients (step 312).

20 **Process of Decrypting an Encrypted Email Message**

FIG. 4 is a flow chart illustrating the process of decrypting an encrypted email message 104 at a recipient 110 in accordance with an embodiment of the present invention. Recipient 110 starts by receiving email message 104 generated by sender 102 (step 402). Next, recipient 110 attempts to match key IDs 210-212 (from recipient block 204 in email message 104) with public keys corresponding to the private keys 114 held by recipient 110 (step 404).

If a public key matches a key ID, for example say a public key held by recipient 110 matches truncated key ID 212, recipient 110 decrypts the corresponding encrypted session key 218 with the private key corresponding to the matching public key. This restores the session key. Recipient 110 then

5 decrypts encrypted message body 206 using the restored session key, and then verifies that the checksum 208 is properly formed from the message body (step 406). Verifying the checksum additionally verifies that the proper private key was used to restore the session key.

If more than one public key held by recipient 110 matches a key ID in

10 recipient block 204, recipient 110 may have to repeat this decryption and verification process for more than one public key.

The foregoing descriptions of embodiments of the invention have been presented for purposes of illustration and description only. They are not intended to be exhaustive or to limit the present invention to the forms disclosed.

15 Accordingly, many modifications and variations will be apparent to practitioners skilled in the art. Additionally, the above disclosure is not intended to limit the present invention. The scope of the present invention is defined by the appended claims.